Technology Control Plan

By

Michael Swansburg,
U.S. Security Professional

[The following article is a reprint from the *Counterintelligence News and Developments*, Volume 1, March 2000.]

Introduction

As more U.S. contractors are expanding from their traditional roles in the U.S. government arena into commercial ventures, they are increasing their contacts with foreign entities. These contacts take the form of joint ventures, joint research, hiring foreign national employees, and hosting foreign visitors. In addition, international inspections associated with agreements such as the chemical weapons treaty and the international standards protocols can expose companies to visits by foreign technology experts. By expanding their contacts with foreign entities, U.S. government contractors are increasing their vulnerability to the potential loss of classified, proprietary, and export-controlted information. The implementation of a technology control plan can significantly mitigate this increased vulnerability.

Technology Control Plan

A technology control plan (TCP) stipulates how a company will control its technology. The plan establishes procedures to protect classified, proprietary, and export-controlled information; to control access by foreign visitors; and to control access by employees who are non-U.S. persons. A TCP is a type of security countermeasure frequently overlooked by companies in the rush to secure business in the international marketplace. The *National Industrial Security Program Operating Manua*l (NISPOM) and the *International Traffic in Arms Regulations* (ITAR) may require a TCP under certain circumstances. Thus, your TCP should contain procedures to control access for all export-controlled information.

What should be in a TCP?

A TCP should consist of the following six parts:

- Description of information to be protected. All employees of a company should know what they are required to protect. Although classified information is marked with classification caveats on each page, proprietary information, trade secrets, and export-controlled information are not always well marked or otherwise identifiable to company employees. This could result in the loss of valuable information or an export violation simply by not knowing what to protect.

- Specific measures to control access within the facility. These measures may include badges, escorts, segregated work areas, etc.

- Procedures for control of access to equipment. The act of physically removing classified, proprietary, or export-controlled information from company facilities presents the greatest risk of getting caught by someone who may be attempting espionage. To limit personal

risk, unscrupulous individuals may attempt to use electronic processing and communications devices to facilitate the transfer of massive amounts of data in a short period of time. For this reason, access to equipment such as fax machines, copiers, and automation information systems should be controlled.

- Indoctrination. Once a TCP has been approved, company personnel, including non-U.S. employees, should be trained in their responsibilities. Remember, the definition of a trade secret under the Economic Espionage Act of 1996 states that the owner thereof has taken reasonable measures to keep such information secret. Therefore, as an additional measure, the company imposed penalties for loss of protected information by noncompliance, negligence resulting in compromise or actual theft should be included in the training session and spelled out in a company document.

- Certification signed by non-U.S. persons. Once non-U.S. employees have been briefed about their responsibilities, they should sign an agreement with the company that they will comply with the security requirements imposed by the company. The agreement should also state what the implications are for not complying with the security requirements. This will eliminate any argument by the individual if caught doing something wrong and using "I didn't know" as an excuse for their actions.

- Designate a company employee responsible for monitoring TCP activities. Finally, someone in the company needs to be responsible for TCP oversight. If a specific employee is not made responsible for monitoring the TCP, it will probably not be adhered to and become an ineffective security countermeasure.

Requirements

Situations involving foreign visitors, foreign employees, joint ventures, and research in which a U.S. government contractor may be required to implement a TCP are listed below:

- Foreign visitors. The contractor shall establish procedures to ensure that foreign visitors are not afforded access to classified information and other export-controlled technical data except as authorized by an export license, approved visit request, or other exemption to the licensing requirements (NISPOM Paragraph 10-507d).

- Foreign employees. A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the cognizant security agency (CSA) determines that procedures already in place at the contractor's facility are adequate. The TCP shall contain procedures to control access for all exportcontrolled information. A sample of a TCP may be obtained from the CSA (NISPOM Paragraph 10-509 and ITAR Section 126.13(c).

A TCP approved by the CSA shall be developed and implemented by those companies cleared under a voting trust agreement, proxy agreement, special security agreement, and security control agreement or when otherwise deemed appropriate by the CSA. The TCP shall prescribe all security measures determined necessary to reasonable foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized. The TCP shall also prescribe measures designed to ensure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate federal government disclosure authorization has been obtained - for example, an approved export license

or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures shall be included, as appropriate (NISPOM Paragraph 2-310).

- Joint ventures and joint research. Extended visits and assignments of foreign nationals to contractor facilities shall be authorized only when it is essential that the foreign national be at the facility pursuant to a contract or government agreement (for example, joint venture, liaison representative to a joint or multinational program, or direct commercial sale) (NISPOM Paragraph 10-508a).

The applicable CSA shall be notified in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities. This notification shall include a copy of the approved visit authorization or the U.S. government export authorization arid the TCP (NISPOM Paragraph 10-508c).

Conclusion

Access by foreign nationals to U.S. government and commercial contractor facilities greatly increases the risk of losing classified, proprietary and export- controlled information. The security countermeasures a company puts in place should be tailored to its operations and to the specific threats identified. Counterintelligence organizations can help identify specific threats. A TCP is a good security countermeasure for mitigating vulnerabilities associated with these increased risks. In many cases, a TCP will be required and in other cases it is just sound business practice for the company to implement a TCP. Whenever you feet a TCP is either require or right for your company, a trained security professional can help you develop the right plan.

About the Author

Michael Swansburg is a security professional with over twenty years of counterintelligence and industrial security experience as a military intelligence officer and government civilian.